Remarks

This reply is responsive to the Office communication mailed January 25, 2005. Page and paragraph references are to that communication unless otherwise indicated.

Claims 1-19 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Taaffe 4,747,139 ("Taaffe") and further in view of Glowny et al. 5,537,642 ("Glowny") (page 2, ¶ 2). Additionally, claims 2-3, 6-11 and 13-14 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Taaffe and Glowny as applied to claim 1 and further in view of Schneier, Applied Cryptography ("Schneier") (page 4, ¶ 9). Applicants respectfully traverse.

Applicants' invention relates to a method, apparatus, and program storage device for controlling the transition of a cryptographic system (crypto module 102) having one of a plurality of security-relevant states from an existing state to a future state under control of one or more authorities (104). In accordance with the invention, the system stores control information (signature requirement array 156) specifying permissible future states based on a current state and a requesting authority. In response to receiving a query (114) from an authority as to the current state of the system, the system provides a reply (124) to the authority that contains nonsecret state information (signed portion 128) regarding the current state of the system and reply authentication information (signature 126) for enabling the authority to determine whether the reply originated from the system.

The system may also receive a request (command 116) from an authority to change the current state of the system. The request contains state change information (command data) indicating a proposed future state of the cryptographic system and request authentication information (signature 118) for enabling the system to determine whether the request originated from the authority. Upon receiving such a request, the system determines using the request authentication information whether the request originated from the authority (step 1004). The system performs the request (step 1012) only if the request is determined to have originated from the authority and the proposed future state is a permissible future state as specified by the control information (step 1010).

Taaffe discloses a software security method and apparatus in which an input key 30 (Fig. 1A) is applied to a physically secure key generator 28—realized as a finite-state machine (FSM) (Fig. 2)—to generate an output key 26. An encryptor 22 uses the output key 26 to encrypt data 20 to produce encrypted data 24. The encrypted data 24 is stored along with the input key 30 on a storage medium 32. A corresponding decryption scheme is shown in Fig. 1B. Using the retrieved input key 40 from the storage medium 32, key generator 28 regenerates an output key 38 identical to the original output key 26. A decryptor 34 (erroneously labeled as an encryptor in the figure) uses output key 38 to decrypt the encrypted data on the storage medium 32 to regenerate the original input data as an output 36. The key generator 28 and an encryptor/decryptor 60, 70 are used in an otherwise conventional computer containing a CPU 50 (Figs. 6 and 7).

The Examiner argues that Taaffe discloses applicants' claimed invention except for the authentication steps, that Glowny teaches these steps, and that it would have been obvious to have modified Taaffe's system using Glowny's teaching of authenticating information exchanged between processors "to prevent an attacker from intercepting or changing commands being processed in route between the processors" (page 3, ¶ 4). Applicants respectfully disagree.

Contrary to the Examiner's apparent assertion, Taaffe does not disclose applicants' claimed system except for the authentication steps. Given the functional dissimilarity between applicants' claimed system and Taaffe's system, it is not always easy to discern just how the Examiner is matching up the two. However, as best as applicants can determine, the Examiner is making these analogies:

Applicants' Invention	**Taaffe**
Cryptographic system	Key generator 28 (or key generator 28 and encryptor/decryptor 60)
Security-relevant states	FSM states (Fig. 2); encrypted and unencrypted states of input data
Existing state	Unencrypted data 20
Future state	Encrypted data 24

Authority	CPU 50
Control information	Keying information
Query	Task provided by CPU to FSM microprocessor
Reply	"Status messages" from FSM
State-change request	Encryption request

While this analysis produces an apparent reading of applicants' claims (except for their authentication aspects) onto Taaffe, it is not a coherent reading, for the reasons noted below.

Considering first the query aspect of applicants' claimed invention, in applicants' claimed system the reply provided to an authority in response to a query contains nonsecret state information regarding the current state of the cryptographic system. In Taaffe's system, on the other hand, the state of the FSM must be kept secret to ensure the security of the encryption procedure. Further, while the Examiner refers to "status messages" provided by the FSM, applicants are unable to find any reference to such messages in the patent, and any such messages would indicate the completion of a task rather than a security-relevant state of the system as claimed by applicants.

The Examiner counters (¶ 20, pages 6-7) that Taaffe teaches that "only the particular output key word sequence utilized in the encryption" need be held secret. If this statement is meant to imply that the internal state information need not be kept secret, then it is clearly wrong, since it is this internal state information which, together with the input key 30 (a public value), determines the output key 26. Thus, if this state information becomes public, so will the output key.

Considering now the state-change aspect of applicants' claimed invention (the final three steps of claim 1 and the corresponding elements of claim 12) in applicants' system the request from the authority contains state change information indicating a proposed future state of the system. This request is performed by the system only if proposed future state is a permissible future state as specified by the control information.

With the substitutions indicated by the above table, the Examiner is in effect saying that in Taaffe, the key generator 28 and encryptor/decryptor 60 receive a request from the CPU 50 to change the current state of the input data from unencrypted to encrypted, and that these elements perform the request only if the proposed encrypted state of the data is a permissible future state as specified by the keying information. Several things are wrong with this analysis.

In the first place, the encrypted and unencrypted states are states of the input data, not states of the cryptographic system[1] (i.e., Taaffe's key generator and encryptor) as claimed by applicant. Thus, there is no indication in Taaffe that any memory of the input data survives in the encryptor, once the latter has encrypted the data and sent it on to the storage medium. It certainly wouldn't survive in the key generator, since it is never presented to that component in the first place.

Also, the particular encrypted state of the data is determined by the encryption key and input data, without any involvement of the CPU (except possibly for supplying initial seed values to the key generator). This encrypted state is not a "proposed future state" that is contained in state change information received from an "authority", as claimed by applicants. To say otherwise is to suggest in effect that the CPU is giving the encryptor the encrypted data.

Finally, the keying data is not "control information" that specifies "permissible future states based on a current state and a requesting authority". More particularly, even if the keying data is regarded as "control information", it does not specify permissible future states. Rather, the keying data merely provides an encryption key for the input data. While it may determine the future state of the input data, it does not specify whether such a future state is permissible and so does not specify permissible future states. Nor does it specify such states "based on a current state and a requesting authority" as claimed by applicant, since the identity of the authority (or number concurring) is irrelevant.

[1] The Examiner has also equated applicants' states with Taaffe's FSM states, so the Office position here is not altogether clear.

From the foregoing it is apparent that, even without request authentication, Taaffe differs strikingly from applicants' claimed system. Accordingly, even if such authentication were added as allegedly taught by Glowny, one would not obtain applicants' claimed system. Claims 1-19 as amended are therefore respectfully believed to distinguish patentably over the art cited by the Examiner.

Entry of this reply and reconsideration of the application in the light of the above remarks are respectfully requested. It is hoped that upon such consideration the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,
RONALD M. SMITH, SR. et al.

By _____

William A. Kinnaman, Jr.
Registration No. 27,650
Phone: (845) 433-1175
Fax: (845) 432-9601

WAK/wak